diploweb.com La revue géopolitique
ISSN : 2111-4307

La cyberdéfense militaire française à l'épreuve des Jeux Olympiques et Paralympiques de 2024

dimanche 7 janvier 2024,par Sébastien BAPTISTE

Citer cet article / To cite this version :
Sébastien BAPTISTE, **La cyberdéfense militaire française à l'épreuve des Jeux Olympiques et Paralympiques de 2024**, *Diploweb.com : la revue géopolitique, 7 janvier 2024.*

Le cyberespace est le théâtre d'une guerre permanente. C'est aussi le support principal des échanges sociaux et économiques, faisant de chaque cyberattaque un facteur de déstabilisation du quotidien. Les Etats et les groupes organisés qui y ont recours font preuve de toujours plus d'audace, frappant avec une apparente impunité. La défense semble désavantagée du fait de son coût d'installation et de mise en œuvre mais surtout, elle n'a pas l'initiative. Un adversaire n'a besoin que d'une faille et choisit quand il l'exploite. Le défenseur doit surveiller l'entièreté de son périmètre, et ce constamment. Les systèmes militaires ne sont pas épargnés, et font quotidiennement objets d'actions malveillantes. A l'approche des Jeux Olympiques et Paralympique de 2024 (JOP 2024), cet article vise à identifier les enjeux de la cyberdéfense militaire dans la préparation aux menaces de demain.

LORS de ses vœux aux armées du 20 Janvier 2023 à Mont-de-Marsan, le président Emmanuel Macron a annoncé un effort majeur dans le domaine militaire en dessinant les orientations de la future Loi de programmation militaire (LPM) 2024-2030. Les armées disposeront de 413 milliards d'euros entre 2024 et 2030, soit **128 milliards de plus que la LPM 2019-2025**. Après la « réparation », effet majeur de la LPM actuelle, le président veut une « transformation » autour de quatre pivots, pour adapter les moyens des forces armées aux dangers de demain.

Dans le premier de ces pivots, il évoque la cyberdéfense. Plus précisément, le président annonce vouloir « doubler [la] capacité de traitement des attaques cyber majeures » [1]. Cette ambition aux accents militaires fait écho au volet cyber de France 2030, qui prévoit « d'allouer plus d'un milliard d'euros afin de faire de la France une nation de rang mondial dans la cybersécurité » [2]. La concordance de ces mesures civiles et militaires témoigne de la prise de conscience généralisée, bien que tardive, d'une menace grandissante envers les intérêts français dans le cyberespace.

Cet article présente la cyberdéfense militaire dans la perspective des JOP 2024, et détermine comment celle-ci pourra faire face aux attaques futures. Après une étude générale des attaques et de la défense dans le cyberespace, l'article identifie et traite deux enjeux : la coordination des unités de cybersécurité et l'augmentation en nombre de personnel qualifié.

I. L'évolution du cyberespace, de l'attaque à la défense

Le cyberespace est le support de la société sous toutes ses facettes, en particulier sociale et économique. Les données et les ressources qu'il héberge sont donc naturellement les cibles d'acteurs malveillants. Cette tendance étant vouée à s'accroitre, investir dans la cybersécurité relève de la nécessité.

Des attaques toujours plus nombreuses contre les entités gouvernementales

Les attaques informatiques sont toujours plus nombreuses, insidieuses et dévastatrices. Elles ont occasionné deux milliards d'euros de dégâts pour l'économie française en 2022, selon une étude d'Asterès [3]. Baromètre gouvernemental créé par l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), la plateforme cybermalveillance.gouv.fr note des hausses de 54% sur les attaques par hameçonnage (méthode pour obtenir du destinataire d'un courriel

des informations confidentielles) et de presque 100% sur le piratage de compte entre 2021 et 2022. Elle note néanmoins une baisse de 16% du nombre d'attaques par rançongiciel.

Les systèmes d'information gouvernementaux et militaires sont des cibles de choix. En effet, ils collectent les données de leurs utilisateurs (citoyens, patients, militaires), lesquelles ont une grande valeur marchande. Une fois piratées, elles sont régulièrement en vente sur le *Darkweb* après l'habituelle tentative d'extorsion. Au-delà de l'appât du gain, les attaques contre des entités gouvernementales ou militaires visent aussi à obtenir du renseignement et du sabotage.

L'attribution d'une attaque est compliquée, son coût est relativement faible et les effets obtenus potentiellement critiques. Logiquement, les acteurs étatiques et les groupes organisés qui y ont recours ont augmenté leurs activités dans cette branche. L'invasion de l'Ukraine par la Russie marque une intensification historique dans la contestation d'un monopole occidental sur la marche du monde. Le cyberespace en est un champ de conflictualité : un rapport de Mandiant note une augmentation de 250% des cyberattaques russes contre l'Ukraine en 2022 par rapport à 2020, et de 300% contre les pays de l'OTAN sur la même période [4].

Bien sûr, ces statistiques sont biaisées car seules les cyberattaques découvertes sont comptabilisées. Leur proportion vis-à-vis de la totalité des cyberattaques est difficilement quantifiable, et ce d'autant plus que la tendance des adversaires est de favoriser la discrétion. Le rapport des menaces 2022 de l'ANSSI décrit un adversaire « toujours plus performant » cherchant désormais davantage « des accès discrets et pérennes » [5].

La cybersécurité, effet stratégique majeur

Conscients de l'enjeu, les acteurs civils et militaires ont renforcé les trois piliers de la cybersécurité : cyberrésilience, cyberprotection et cyberdéfense.

Premières lignes de défense, la cyberprotection et la cyberrésilience sont des priorités nationales. La cyberprotection augmente le niveau de sécurité par la sensibilisation des utilisateurs, la gestion du chiffre, la réglementation et les homologations. Elle repose aussi sur une veille technologique pour connaitre les failles découvertes et les corriger sur son périmètre. La cyberrésilience permet à un système attaqué sinon de continuer son service pendant une attaque, du moins de rapidement se remettre des dégâts occasionnés. Dans une logique de défense en profondeur, la cyberdéfense décèle et met fin à une attaque en cours. Les unités de renseignement jouent un rôle crucial dans le cyberespace. En amont d'une attaque, ils traitent le renseignement d'intérêt cyber (RIC) sur les adversaires de la France et sur leurs modes opératoires d'attaque (MOA). Pendant et après l'attaque, ils collectent le renseignement d'origine cyber (ROC), c'est-à-dire les éléments techniques de l'attaque. Selon le président Macron lors de son discours à Mont-de-Marsan, la loi de programmation militaire pour 2025-2030 augmentera le budget des unités de renseignement de 60% à 100% [6].

Il faut noter que toutes ces spécialités cyber souffrent d'un manque en ressources humaines. En 2021, le cabinet Wavestone estimait que 15 000 postes étaient à pourvoir dans ce domaine en France, et 3,5 millions dans le monde. Le recrutement est le principal défi de la LPM 2024-2030 ; nous y reviendrons.

La multiplication des incidents cyber

Notre environnement physique est marqué par une numérisation croissante. Appelé « Tout connecté » dans le monde civil et Numérisation de l'Espace de Bataille (NEB) par l'Armée de Terre, ce phénomène augmente la surface d'attaque des systèmes d'information. Il faut aussi considérer l'augmentation du nombre d'attaques, ainsi que l'intensification des efforts consacrés à la cybersécurité et au renseignement. Dans l'intervalle 2024-2030, il est probable que les défenseurs trouveront plus fréquemment les adversaires ayant compromis des systèmes d'informations militaires qu'auparavant.

Facteur aggravant, la France accueille un évènement d'envergure mondiale qui attire les cyberattaques : les Jeux Olympiques et Paralympiques de 2024 (JOP 2024). L'évènement mondial est une cible récurrente pour **porter atteinte à l'économie, à la stabilité et au prestige du pays hôte**. Malgré le caractère civil de cet évènement, plusieurs éléments laissent penser que la cyberdéfense militaire est susceptible de porter assistance à des défenseurs civils si ceux-ci viennent à être débordés. Cette hypothèse s'appuie sur les déclarations du chef d'état-major des armées (CEMA) [7] , sur la LPM 2024-2030 qui prévoit « un appui militaire à l'ANSSI en cas de crise cyber majeure » [8] mais aussi sur la « règle des 4i », c'est à dire les conditions pour mobiliser des moyens militaires lorsque les moyens civils sont « indisponibles », « insuffisants », « inadaptés » voire « inexistants ».

> Quel meilleur moment pour porter atteinte aux instances gouvernementales ou militaires que celui où ses défenseurs sont déjà débordés ?

Un **scénario catastrophe** dans le cyberespace pendant les JOP est tout à fait envisageable. Les organisateurs de la session de 2016 à Rio ont dénombré plus de 50 millions d'attaques, selon un article du *Point* du 12 juillet 2023 [9]. Ceux de Tokyo en 2021 en ont signalés plus de 350 millions, et Bruno Marie-Rose, directeur de la technologie de Paris 2024, s'attend à un nombre 8 à 10 fois supérieur : au moins 3 milliards de cyberattaques. D'après le retour d'expérience des deux dernières sessions, il faut s'attendre à des tentatives de piratages de sites gouvernementaux, des attaques par dénis de service et des attaques par rançongiciel. Il faut aussi anticiper des attaques plus évoluées, voire étatiques : **quel meilleur moment pour porter atteinte aux instances gouvernementales ou militaires que celui où ses défenseurs sont déjà débordés ?**

Comme le rappelait le général Bonnemaison devant la commission de la défense nationale et des forces armées le 7 décembre 2022, « la fulgurance des attaques ne doit pas masquer leurs délais incompressibles de conception et de planification. Il faut des mois, voire des années pour construire une cyberattaque » [10]. L'échéance des JOP 2024 approche, et ceux qui projettent des attaques cyber contre la France à cette occasion sont donc **déjà en train de de tester leurs outils et de sonder les défenses**.

II. La coordination cyber : en deçà de l'enjeu stratégique, un défi tactique

La cyberdéfense militaire française est caractérisée par la diversité des acteurs sur lesquels

elle repose. Bien que disposant d'une chaine de commandement et d'organisme de coordination au niveau opérationnel, la condition de son efficacité est une coordination au plus proche de la victime.

Préparer un incident grâce à la cybersécurité et aux partenariats

D'après Sébastien Vincent, adjoint au COMCYBER en 2023, une stratégie de dissuasion cyber vise à décourager en imposant « un coût suffisant à l'adversaire pour le faire renoncer à son entreprise malveillante par le déni et/ou la crainte de la punition. » [11]. L'expérience montre que cet objectif est partiellement atteint, car l'adversaire est contraint de s'adapter aux efforts des défenseurs. Cette défense se forme sur plusieurs niveaux, et dans tous les temps d'une cyberattaque. Cet article se restreindra au niveau tactique qui met davantage en œuvre les actions de déni que de punitions.

Sur le temps long, en amont d'un incident, le Centre de Coordination des Crises Cyber (C4) permet « une analyse partagée […] de la menace, des modes d'action et des acteurs menaçants » [12]. En d'autres termes, grâce à une coopération nationale des acteurs du cyberespace, les attaques connues de l'un doivent devenir rapidement inefficaces contre tous.

L'attaquant doit donc dissimuler ses actions et de se réinventer régulièrement sous peine d'être détecté, identifié et contré au niveau national. Les cybercombattants assurent une veille permanente des réseaux du ministère des Armées, qui contiennent plus de 300 000 machines réparties dans le monde entier [13]. La défense s'appuie sur un maillage de *Security Operation Centers* (SOCs), c'est-à-dire de plateformes qui assurent la supervision et l'administration de la sécurité du système d'information. Lorsqu'un SOC confirme la compromission d'un système militaire, il y répond avec une réaction de premier niveau pour gêner les actions de l'adversaire. Dans la revue Transmetteurs [14], l'article dédié à la 807e compagnie de transmissions, le SOC de l'Armée de Terre, précise que cette unité déploie « plus de 600 contre-mesures par an », pour faire face à « une attaque [majeure] tous les dix jours en moyenne » sur les systèmes français du théâtre sahélo-saharien.

Au plus proche des systèmes, la cyberprotection participe à la dissuasion en augmentant la difficulté d'une attaque. Le budget du COMCYBER lors de la LPM 2019-2024 s'est porté à 60% sur le chiffre, pour réparer une dette historique qu'un rapport du Sénat évalue à un milliard d'euros [15]. Infiltrer un système dont les utilisateurs sont avertis, dont les risques sont connus et surtout maitrisés impose de créer une attaque « sur mesure ». Ce type d'attaque est complexe, long à produire et difficilement réutilisable sur une autre cible.

Si l'attaque nécessite une expertise supplémentaire à celle du SOC pour être contrée, le COMCYBER peut ordonner le déploiement rapide de matériel et de personnel formé à la réponse à incident. Ce dispositif prend le nom de Groupe d'Intervention Cyber (GIC), et peut être projeté aussi bien en métropole qu'à l'étranger. Il est armé principalement par le Centre d'Analyse en Lutte Informatique Défensive (CALID), le centre d'alerte et de réaction aux attaques informatiques des Armées, qui dispose des moyens matériels, des compétences techniques et de l'expérience opérationnelle nécessaires à la réponse aux incidents majeurs.

Figure 1 : Actions des défenseurs face à une cyberattaque

La réponse à incident : reprendre l'ascendant par tous les moyens

Les unités de la cyberdéfense et du renseignement disposent de capacités complémentaires indispensables à la réponse à incident. Elles échangent de façon hebdomadaire au niveau opérationnel et mensuelle au niveau stratégique dans le cadre du Centre de Coordination des Crises Cyber (C4) [16]. Lors d'une réponse à incident, ce cadre trouve ses limites car les capacités doivent être mises en œuvre localement et dans un délai bien plus restreint pour gêner efficacement l'adversaire.

Le chef de GIC coordonne ces capacités au plus proche du système attaqué. Officier subalterne ou personnel civil, il encadre un groupe de spécialistes et s'adapte aux situations de crises cyber avec un raisonnement tactique. Maillon entre les analystes au niveau technique, les décideurs au niveau opérationnel et les responsables du système attaqué, le chef de GIC décline les ordres à son groupe, synthétise la situation, coordonne les appuis et assure la liaison avec les responsables du système.

Le GIC doit tout d'abord découvrir l'environnement dans lequel il va combattre. Il arrive que l'administration locale ne puisse pas fournir une vue précise de son système. Des auditeurs du Centre d'audit en Sécurité des Systèmes d'Information (CASSI) peuvent appuyer le GIC, de par leur capacité à lister les vulnérabilités et à cartographier le système attaqué.

Après avoir cartographié le terrain, il faut être en mesure de détecter les actions malveillantes sur le système. On peut s'appuyer sur le SOC de l'unité attaquée. Dans sa recherche de l'adversaire sur le système, le GIC peut être appuyé par des analystes en investigations numériques et en rétro-ingénierie du CALID.

En 2019, la France s'est officiellement dotée d'une doctrine de lutte informatique offensive (LIO). Le GIC pourrait donc être appuyé par des actions de lutte informatique offensive, **dirigées contre l'architecture de l'adversaire dans le but de de « recueillir ou d'extraire des informations », voire de « neutraliser les capacités adverses » pour contraindre l'adversaire à arrêter ses attaques** [17].

Tout au long de l'attaque, le GIC collecte des éléments techniques et les transmet à l'appui de *Cyber Threat Intelligence* (CTI). Cet appui collecte et traite les informations sur les menaces ou les acteurs de la menace, qu'il diffuse par le C4 et échange dans le cadre de partenariats. « **C'est l'une des leçons de l'Ukraine : lorsque l'on est attaqué, l'échange de données**

techniques est essentiel. » déclarait le général Bonnemaison en avril 2023 [18]. En retour, le GIC peut recevoir ce que le C4 ou les partenaires savent des éléments techniques. Ces informations permettent de faire avancer l'investigation du GIC.

Enfin, le GIC peut modifier le champ de bataille par l'action des administrateurs. Pour gêner l'adversaire, il peut éteindre des machines, bloquer des flux, changer des configurations. Les possibilités sont nombreuses et l'adversaire peine à distinguer une action défensive expérimentée d'un innocent problème technique.

Le rôle du chef de GIC prend toute son importance dans la gestion d'un incident majeur, où tous ces appuis sont mobilisés. Non content de maitriser l'investigation numérique et les actions de lutte informatique défensive (LID), il doit être familier avec les techniques et les besoins des appuis pour les intégrer dans sa manœuvre. Grâce à une coordination des différents effets, la défense reprend l'ascendant sur l'attaque. Cette compétence demande une formation et un entrainement régulier au profit des chefs de GIC.

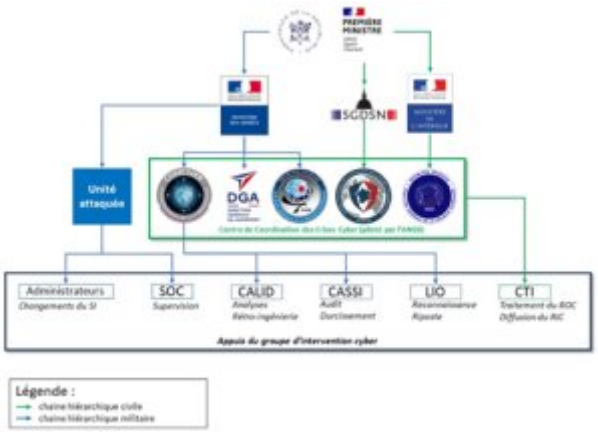

Figure 2 : chaines hiérarchiques des appuis lors d'une réponse à incident sur un système militaire

Exploiter l'incident en dévalorisant les atouts de l'adversaire

Une fois l'incident terminé, les efforts en matière de cyberrésilience permettent de remettre rapidement en service tout système endommagé, réduisant ainsi les conséquences de l'attaque. Idéalement, ce dernier n'a jamais été interrompu, grâce à des sauvegardes et des redondances mises en place en amont de l'incident.

Le GIC transmet le renseignement d'origine cyber (ROC) généré pendant les investigations à son appui CTI, qui le traite et le diffuse sous forme de RIC. Cette diffusion participe à la dissuasion, car elle rend inefficace les outils et les méthodes de l'adversaire sur les systèmes des partenaires. Le RIC peut contenir des empreintes cryptographiques, mais aussi les adresses IP et les noms de domaines malveillants, voire des outils que le GIC a extrait du système attaqué. Les partenaires peuvent ainsi s'assurer qu'ils ne sont pas victimes de la même attaque et s'en prémunir dans le futur.

L'idéal reste de s'en prendre aux techniques, tactiques et procédures (TTP), pour monter aussi haut que possible dans l'échelle de la cyber-douleur [19]. Par exemple, protéger la messagerie d'une entreprise contre la technique du hameçonnage force des adversaires spécialisés dans

cette technique à choisir entre en développer une autre pour infiltrer, ou chercher une autre cible moins bien protégée.

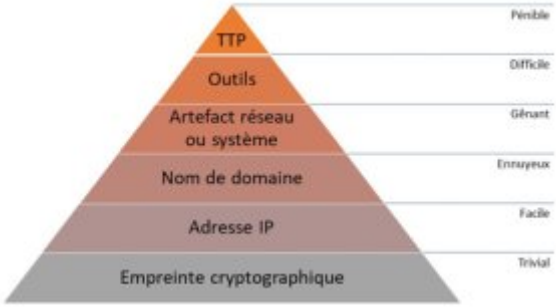

Figure 3 : Echelle de la cyber-douleur
Légende : Atouts de l'adversaire à gauche, douleur engendrée par les contre-mesures à droite.

« Les cyberattaques ont pour caractéristique une facilité à traverser les frontières et à brouiller les limites entre niveaux d'analyse sociétal, gouvernemental et international » notait Joe Burton en 2018 [20]. Il est donc nécessaire d'échanger des informations efficacement entre entités privées, gouvernementales et militaires non seulement au niveau national, mais aussi international. Dans le prolongement d'une Europe de la Défense, **une cyberdéfense européenne serait un bouclier plus efficace que les cyberdéfenses nationales plus ou moins bien coordonnées, entravées par leur diversité**.

> L'attribution est la marque de la puissance dans le cyberespace.

Le but ultime de la cyberdéfense est de fournir suffisamment d'éléments techniques pour que les unités de renseignement puissent imputer l'attaque, c'est-à-dire d'en **identifier l'origine et les commanditaires avec suffisamment de certitude pour que les autorités politiques l'attribuent publiquement. « Cette capacité d'attribution est la marque de la puissance dans le cyberespace »**, selon Thomas Gomart [21]. L'attribution d'une cyberattaque est toujours délicate et reste un geste politique fort que la France n'a effectué que trois fois : pour dénoncer la Russie en 2019 [22], indirectement la Chine en 2021 [23] puis à nouveau la Russie en 2022 [24].

III. Le personnel, principale richesse et principal défi

Au même titre que les entreprises privées, les unités de la cyberdéfense militaire anticipent des besoins accrus en personnel malgré un marché sous tension. Disposant d'avantages qui lui sont propres, ces unités doivent attirer et fidéliser pour honorer des objectifs de recrutements conséquents.

Contrainte de la particularité militaire sur le niveau tactique

Aussi sophistiquée que puisse être la cyberdéfense militaire, sa puissance repose sur le nombre et la valeur de son personnel. **Le recrutement, la formation et l'entrainement des**

analystes sont donc au cœur de la stratégie de cyberdéfense française.

Le recrutement de l'échelon technique est en partie direct, grâce, par exemple, au brevet technique supérieur (BTS) cyber de Saint-Cyr l'Ecole ou aux officiers sous contrat (OSC). La cyberdéfense est aussi accessible par le biais des mutations. Enfin, le recrutement civil permet de répondre rapidement à un besoin particulier pour une durée de service jusqu'à deux fois supérieure à celle d'un militaire. Cet échelon bénéficie d'un budget de formation et d'entrainement conséquent, pour acquérir et conserver un haut niveau d'expertise.

Selon le secrétariat général pour l'administration, le ministère des Armées emploie 25% de civils [25]. **La proportion de civils dans la cyberdéfense est plus importante** du fait de sa technicité, mais elle reste inférieure à celle du personnel militaire. Bien que servant sous un commandement interarmées, chaque militaire de la cyberdéfense reste attaché à son armée d'origine. En particulier, la politique de mutation oblige tout cybercombattant à changer régulièrement de lieu d'affectation. A cette dynamique de flux historique s'ajoute la pression des conditions avantageuses proposées par les acteurs privés de la cyberdéfense, qui charment chaque année quelques analystes de la cyberdéfense militaire.

Affectations, mutations et départs anticipés font du personnel militaire **une population sans cesse changeante, qu'il faut continuellement accueillir, former, entrainer puis laisser partir**. Une politique rigoureuse de gestion des compétences au niveau opérationnel est nécessaire pour que les centres de cyberdéfense puissent **conserver le haut degré de technicité et la disponibilité que réclament leurs missions**. La tâche est rude : au CALID, en 2021, 20% du personnel était pris par les formations [26]. Considérant le triplement du budget de formation avec la nouvelle LPM [27], et en ajoutant l'entrainement, les missions de routine et les permissions, où trouver le temps de répondre à deux fois plus de crises cyber majeures, comme l'annonçait le président Macron [28] ? C'est pourtant la mission principale du CALID sur le périmètre des armées.

L'augmentation des effectifs est donc inévitable pour espérer faire face aux menaces à venir. Le COMCYBER a pour objectif de recruter 1 800 cybercombattants supplémentaires entre 2023 et 2025 [29].

Les niveaux tactiques et opérationnels de la cyberdéfense

L'échelon tactique est armé par des officiers subalternes ou par des civils expérimentés. Le recrutement de cet échelon dépend principalement de la candidature sur les fiches de poste publiées par le ministère des Armées. Ces recrues spontanées, par nature variables d'année en année, n'ont pas toutes l'appétence ou les compétences pour être chefs tactiques. **Réserver quelques places en sortie des grandes écoles de commandement**, à l'image de l'armée de l'air et de l'espace, assurerait l'arrivée stable de jeunes cadres promis à des carrières longues dans la cyberdéfense militaire. C'est une perspective incontournable dans une spécialité qui espère compter 5200 cybercombattants sur ses rangs en 2025 [30]. De cet échelon sont issus les chefs de GIC, dont le rôle central dans la réponse à incident a été démontré plus haut.

Une formation uniformisée permettrait aux cadres de la cyberdéfense d'acquérir **une culture de la cyberdéfense**. A l'occasion de la passation de commandement du GCA le 18 juillet 2023,

le général Bonnemaison a annoncé la création d'une **académie de cyberdéfense** visant à « coordonner les formations pour faire monter en gamme [ses] cadres » [31].

L'entrainement de l'échelon tactique est assuré grâce aux efforts du C2PO (Centre Cyber de Préparation Opérationnelle). Néanmoins, les occasions d'entrainer les différentes unités de la cyberdéfense à travailler conjointement sur un même incident sont rares. L'exercice DEFNET fournit la plus importante, donnant aux cybercombattants un terrain de jeu et des missions à l'échelle d'une armée dans le cadre de l'exercice ORION.

L'échelon opérationnel de la cyberdéfense assure la conduite des actions de lutte informatique défensive. Cet échelon est armé par des officiers supérieurs ou des civils. L'arme cyber étant relativement jeune, le personnel militaire de cet échelon n'est pas toujours issu de la cyberdéfense. Le master en gestion des crises cyber de Saint-Cyr offre une initiation dans la cyberdéfense pour ceux dont la première partie de carrière a eu lieu dans une arme plus conventionnelle, mais cette formation ne remplace pas l'expérience. De la future académie de cyberdéfense sortira la première génération de cadres aptes à inscrire leur action dans un dispositif cyber complexe. Elle armera à terme les échelons opérationnels puis stratégiques.

Organisé par l'Agence Européenne de Défense (AED), l'exercice annuel MilCERT Interoperability Conference (MIC) permet depuis aux équipes de réponse à incident militaires européennes davantage d'interopérabilité aux niveaux tactiques et opérationnels. Toutefois, au même titre que l'exercice américain Cyberflag, il met en avant une disparité importante en termes d'outils, de méthodes et de procédures qui entravent une défense commune coordonnée.

Attirer et fidéliser un personnel qualifié

La politique de recrutement et de mutation du personnel militaire est une inquiétude constante pour les unités de cyberdéfense. Il est impossible de recruter uniquement des civils déjà qualifiés et expérimentés, faute de pouvoir s'aligner sur les salaires privés mais aussi à cause des contraintes opérationnelles de la cyberdéfense militaire. Gardes, astreintes et opérations extérieures impliquent que plus de la moitié des effectifs doivent être militaires et donc imposées par les ressources humaines des trois armées. Celles-ci souffrent d'ailleurs de la même carence dans les spécialités informatiques.

Cette carence peut être partiellement compensée par une maturité organisationnelle, qui capitalise l'expérience en l'intégrant dans le fonctionnement même de l'unité. Le statut d'officier commissionné, plus souple que celui de carrière ou d'OSC dans son emploi, est une solution complémentaire pour honorer les places militaires par un recrutement civil [32] mais aussi pour conserver quelques années supplémentaires le savoir-faire des sous-officiers désireux de reconversion.

Prenant la mesure d'un marché en forte tension, les Armées se tournent également vers les sorties d'écoles. En témoignent la création d'une classe de BTS cyber à Saint-Cyr l'Ecole, le doublement de ses effectifs à la rentrée 2023 [33], l'inauguration du pôle d'excellence cyber (PEC) en Bretagne ou encore le partenariat avec l'Ecole Polytechnique annoncé dans la LPM 2024-2030. Le COMCYBER multiplie les actions de communication (comme la participation étudiante à DEFNET [34] et le concours Passe Ton Hack [35]) pour **atteindre un objectif de recrutement titanesque**.

Il ne suffit pas de recruter, encore faut-il fidéliser. Les armées disposent de leviers efficaces pour valoriser les cybercombattants. A titre d'exemple, la prime de lien au service (PLS) est accordée depuis 2020 aux OSC qui s'engagent dans le domaine cyber [36]. Le COMCYBER mise aussi sur des parcours diversifiés, qui intègrent des passerelles entre ses unités, l'ANSSI et la DGSE [37]. Il s'agit de **proposer une alternative aux conditions avantageuses des entreprises civile**s : les cybercombattants sont deux à trois fois moins bien rémunérés que leurs homologues du secteur privé [38]. Néanmoins, ils y trouvent le service comme moteur de leurs actions, une perspective plus attirante que la rentabilité d'une entreprise. Pour ceux qui s'engagent, sacrifier une partie de son salaire potentiel vaut bien le sentiment quotidiennement renouvelé de servir la Nation.

Conclusion

La cyberdéfense militaire fait face à un large éventail de menaces, qui se dépassent régulièrement en efficacité et en audace. L'effort budgétaire consenti par le gouvernement français témoigne de l'intensité des incidents à venir. Deux enjeux se distinguent à court terme pour que la cyberdéfense militaire française conserve son rang mondial : disposer d'un personnel qualifié en nombre suffisant et développer la coordination des unités de cyberdéfense. A moyen terme, il faudra aussi renforcer la cyberdéfense à l'échelle européenne car les frontières françaises sont poreuses dans le champ immatériel.

Multipliant les efforts dans ces deux axes, la cyberdéfense militaire monte en puissance. Les Jeux Olympiques et Paralympiques de 2024 pourraient bien lui réserver une épreuve dédiée. L'avenir dira si elle y participera en appui de son homologue civil débordé, ou si elle sera prise à partie sur son propre périmètre par des attaques d'opportunité. Une certitude cependant : les cybercombattants font un métier d'avenir.

Plus

Les Cadettes de la Cyber pour encourager les jeunes femmes à s'orienter vers la filière cybersécurité/cyberdéfense

Les Cadettes de la Cyber est un programme du Pôle d'Excellence Cyber (PEC), lancé en 2021.

Il a pour objectif d'**encourager les jeunes femmes à s'orienter vers la filière cybersécurité/cyberdéfense**, en les accompagnant via un parrainage de haut niveau, en leur donnant accès à des formations complémentaires, et à un accompagnement à l'insertion dans la vie professionnelle.

Voir le site des Cadettes de la Cyber

P.-S.

L'auteur s'exprime ici à titre personnel. Sébastien Baptiste sert en qualité d'officier dans l'armée de Terre (France). Diplômé de l'Ecole Spéciale Militaire de Saint-Cyr, il a été affecté au Centre d'Analyse en Lutte Informatique Défensive (CALID) au sein du Commandement de la Cyberdéfense (COMCYBER). Pendant trois ans, il a pris part à des exercices de cyberdéfense internationaux et à des opérations de lutte informatique défensive (LID). Il y a occupé le poste d'analyste en investigations numériques, d'adjoint et de chef de groupe d'intervention cyber (GIC).

Notes

[1] Emmanuel Macron, « Déclaration de M. Emmanuel Macron, président de la République, sur la politique de défense de la France, » 20 Janvier 2023. [En ligne]. https://www.vie-publique.fr/discours/287928-emmanuel-macron-20012023-politique-de-defense.

[2] Ministère de l'Economie, des Finances et de la Souveraineté Industrielle et Numérique, « France 2030 | Le Gouvernement lance une nouvelle vague de l'appel à projets pour soutenir le développement de briques technologiques critiques en cybersécurité, » 16 Juin 2023. [En ligne]. https://www.economie.gouv.fr/files/files/2023/communique_AAP_cybersecurite.pdf.

[3] Asteres, « Les cyberattaques réussies en France : un coût de 2 MDS en 2022, » [En ligne]. https://asteres.fr/site/wp-content/uploads/2023/06/ASTERES-CRIP-Cout-des-cyberattaques-reussies-16062023.pdf.

[4] G. Mandiant, « Fog of War - How the Ukraine Conflict Transformed the Cyber Threat Landscape, » Février 2023. [En ligne]. https://services.google.com/fh/files/blogs/google_fog_of_war_research_report.pdf.

[5] ANSSI, « Un niveau élevé de cybermenaces en 2022, » 2023. [En ligne]. https://www.ssi.gouv.fr/actualite/un-niveau-eleve-de-cybermenaces-en-2022/.

[6] Emmanuel Macron, « Déclaration de M. Emmanuel Macron, président de la République, sur la politique de défense de la France, » 20 Janvier 2023. [En ligne]. https://www.vie-publique.fr/discours/287928-emmanuel-macron-20012023-politique-de-defense.

[7] France Télévisions, « Paris 2024 : "Les armées contribueront" à la sécurité des Jeux olympiques et paralympiques, annonce le chef d'état-major des armées, » 6 Avril 2023. [En ligne]. https://www.francetvinfo.fr/les-jeux-olympiques/paris-2024/paris-2024-les-armees-contribueront-a-la-securite-des-jeux-olympiques-et-paralympiques-annonce-le-chef-d-etat-major-des-armees_5755763.html.

[8] Sénat, « Pour une coordination de la cyberdéfense plus offensive dans la LPM 2024-2030, » 24 Mai 2023. [En ligne]. https://www.senat.fr/rap/r22-638/r22-638-syn.pdf.

[9] Gabriel ATTAL, « JO de Paris 2024 : les organisateurs redoutent des milliards de cyberattaques, » 12 Juillet 2023. [En ligne]. https://www.lepoint.fr/societe/jo-de-paris-2024-les-organisateurs-redoutent-des-milliards-de-cyberattaques-12-07-2023-2528212_23.php.

[10] Assemblée Nationale, « Compte rendu - Commission de la défense nationale, » 13 Avril 2023. [En ligne]. https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/l16cion_def2223064_compte-rendu#.

[11] Sébastien VINCENT, « « Qui s'y frotte, s'y pique. » Une stratégie intégrale pour réduire la subversion cyber, » 28 Septembre 2022. [En ligne]. https://www.cairn.info/revue-defense-nationale-2022-HS3-page-41.html.

[12] Sénat, « Délégation parlementaire au renseignement - rapport d'activité 2019-2020, » 11 Juin 2020. [En ligne]. https://senat.fr/rap/r19-506/r19-50638.html.

[13] Ministère des Armées, « Le commandement de la cyberdéfense (COMCYBER), » [En ligne]. https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber. [Accès le 7 Août 2023].

[14] Armée de Terre, « La 807e Compagnie de Transmissions : le bras armé de la cyberdéfense de l'Armée de Terre, » *Transmetteurs N°28,* p. 25, Janvier à Mars 2021.

[15] Sénat, « Pour une coordination de la cyberdéfense plus offensive dans la LPM 2024-2030, » 24 Mai 2023. [En ligne]. https://www.senat.fr/rap/r22-638/r22-638-syn.pdf.

[16] Sénat, « Délégation parlementaire au renseignement - rapport d'activité 2019-2020, » 11 Juin 2020. [En ligne]. https://senat.fr/rap/r19-506/r19-50638.html.

[17] Ministère des Armées, « Doctrine militaire de lutte informatique offensive (LIO), » 18 Janvier 2019. [En ligne]. https://www.defense.gouv.fr/sites/default/files/ministere-armees/Lutte%20informatique%20offensive%20%28LIO%29.PDF.

[18] Assemblée Nationale, « Compte rendu - Commission de la défense nationale, » 13 Avril 2023. [En ligne]. https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/l16cion_def2223064_compte-rendu#.

[19] David BIANCO, « Echelle de la cyber-douleur, » 1 Mars 2013. [En ligne]. http://detect-respond.blogspot.com/2013/03/the-pyramid-of-pain.html.

[20] Joe BURTON, « Cyber deterrence : a comprehensive approach ?, » CCDCOE, Avril

2018. [En ligne]
https://ccdcoe.org/uploads/2018/10/BURTON_Cyber_Deterrence_paper_April2018.pdf.

[21] Thomas GOMART, L'affolement du monde, CPI Firmin-Didot, 2020.

[22] Jean-Dominique MERCHET, « Florence Parly révèle une cyberattaque très sérieuse contre les Armées, » L'Opinion, 18 Janvier 2019. [En ligne].
https://www.lopinion.fr/secret-defense/florence-parly-revele-une-cyberattaque-tres-serieuse-contre-les-armees.

[23] Elise VINCENT, « La Chine dans le viseur de la France dans le cadre d'une « virulente » cyberattaque, » Le Monde, 22 Juillet 2021. [En ligne].
https://www.lemonde.fr/international/article/2021/07/22/la-chine-dans-le-viseur-de-la-france-dans-le-cadre-d-une-virulente-cyberattaque_6089122_3210.html.

[24] Martin Untersinger, « Guerre en Ukraine : la Russie accusée d'être derrière la cyberattaque ayant visé le réseau du satellite KA-SAT, » 22 mai 2022. [En ligne].
https://www.lemonde.fr/pixels/article/2022/05/10/guerre-en-ukraine-la-russie-accusee-d-etre-derriere-la-cyberattaque-ayant-vise-le-reseau-du-satellite-ka-sat_6125513_4408996.html.

[25] Secrétariat général pour l'administration, « Le recrutement civil, » [En ligne].
https://www.defense.gouv.fr/sga/recrutement-militaire-au-sga/recrutement-civil. [Accès le 01 Août 2023].

[26] Defense-Zone, « Les enjeux stratégiques de la cyberdefense, » 11 Aout 2021. [En ligne]. https://defense-zone.com/blogs/news/les-enjeux-de-la-cyberdefense.

[27] Assemblée Nationale, « Compte rendu - Commission de la défense nationale, » 13 Avril 2023. [En ligne].
https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/l16cion_def2223064_compte-rendu#.

[28] Emmanuel Macron, « Déclaration de M. Emmanuel Macron, président de la République, sur la politique de défense de la France, » 20 Janvier 2023. [En ligne].
https://www.vie-publique.fr/discours/287928-emmanuel-macron-20012023-politique-de-defense.

[29] Linda VERHAEGHE, « Guerre en Ukraine : le RETEX du COMCYBER, » 13 Janvier 2023. [En ligne]. https://operationnels.com/2023/01/13/ukraine-retex-comcyber/.

[30] Ministère des Armées, « Le commandement de la cyberdéfense (COMCYBER), » [En ligne]. https://www.defense.gouv.fr/ema/commandement-cyberdefense-comcyber. [Accès le 7 Août 2023].

[31] Pascal SIMON, « Nouveau commandant, académie : ambitions confirmées pour le groupement de cyberdéfense des armées, » 18 Juillet 2023. [En ligne].
https://www.ouest-france.fr/politique/defense/nouveau-commandant-academie-ambitions-co

nfirmees-pour-le-groupement-de-cyberdefense-des-armees-f07bb856-256f-11ee-8552-e3192c603a14.

[32] Ministère des Armées, « Devenir cybercombattant » [En ligne]. https://www.defense.gouv.fr/comcyber/devenir-cybercombattant. [Accès le 6 Janvier 2024].

[33] DRHAT, « Pour faire face aux enjeux du cyberespace, le BTS Cyberdéfense de Saint-Cyr l'École double ses capacités à la rentrée 2023, » Ministère des Armées, 16 Février 2023. [En ligne]. https://rh-terre.defense.gouv.fr/actualites/item/1258-pour-faire-face-aux-enjeux-du-cyberespace-le-bts-cyberdefense-de-saint-cyr-l-ecole-double-ses-capacites-a-la-rentree-2023.

[34] Ministère des Armées, « Le COMCYBER initie des étudiants au cybercombat, » 22 Mars 2023. [En ligne]. https://www.defense.gouv.fr/ema/actualites/comcyber-initie-etudiants-au-cybercombat.

[35] Bertrand LEMAIRE, « La Cyberdéfense à la découverte des cybertalents de demain, » 16 Mai 2023. [En ligne]. https://www.republik-it.fr/rh/formation/la-cyberdefense-a-la-decouverte-des-cybertalents-de-demain.html.

[36] Guerric PONCET, « Une nouvelle prime pour limiter la fuite des cerveaux de l'armée française, » Le Point, 30 09 2019. [En ligne]. https://www.lepoint.fr/societe/une-nouvelle-prime-pour-limiter-la-fuite-des-cerveaux-de-l-armee-francaise-30-09-2019-2338542_23.php.

[37] Assemblée Nationale, « Compte rendu - Commission de la défense nationale, » 13 Avril 2023. [En ligne]. https://www.assemblee-nationale.fr/dyn/16/comptes-rendus/cion_def/l16cion_def2223064_compte-rendu#.

[38] *Idem*